# ABSTRACT

The invention generally relates to management of cryptographic key generations in an information environment comprising a key-producing side generating and distributing key information to a key-consuming side. A basic concept of the invention is to define, by means of a predetermined one-way key derivation function, a relationship between generations of keys such that earlier generations of keys efficiently may be derived from later ones but not the other way around. A basic idea according to the invention is therefore to replace, at key update, key information of an older key generation by the key information of the new key generation on the key-consuming side. Whenever necessary, the key-consuming side iteratively applies the predetermined one-way key derivation function to derive key information of at least one older key generation from the key information of the new key generation. In this way, storage requirements on the key-consuming side can be significantly reduced.